CLAIMS

1. Optical disk (10) for storing data comprising a decryption module (20), that said module (20) including :

- a memory (22) including at least one secret key (K1) ;
- a cryptoprocessor (21) to decrypt the data (DATA) of said disk (10) from said key (K1), and
- data exchange means (IN_A, OUT_A, VCC_A, GRD_A) for applying the data (DATA) of said disk (10) to the cryptoprocessor (21) and reading the decrypted data of the cryptoprocessor (21).

2. Optical disk according to claim 1, characterised in that said decryption module (20) is a chip with an integrated circuit.

3. Optical disk according to claim 1, characterised in that said decryption module (20) is integrated in a central zone of said disk (10).

4. Optical disk according to claim 1, characterised in that the data exchange means (IN_A, OUT_A, VCC_A, GRD_A) are integrated in a central zone of the disk (10).

5. Optical disk according to claim 1, characterised in that it comprises balancing means (E) for balancing said disk.

6. Optical disk according to claim 1, characterised in that the data exchange means are fitted with contacts.

7. Optical disk according to claim 1, characterised in that the data exchange means are fitted with means for transmitting an energy field.

8. Method for reading a data storage optical disk (10) comprising a decryption module (20), said module (20) including :

- a memory (22) including at least one key (K1) ;
- a cryptoprocessor (21), and
- data exchange means (IN_A, OUT_A, VCC_A, GRD_A),

said method including the following stages :

- an application stage in which the data (DATA) of said disk (10) are applied to the cryptoprocessor (21) via the data exchange means (IN_A, OUT_A, VCC_A, GRD_A),
- a decryption stage in which the cryptoprocessor (21) decrypts the data (DATA) of said disk (10) from said key (K1), and
- an extraction stage in which the decrypted data of the cryptoprocessor (21) are read via the data exchange means (IN_A, OUT_A, VCC_A, GRD_A).

9. Method according to claim 8, characterised in that it comprises an additional stage according to which :

- prior to the decryption stage, the data (DATA) is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocessor interface (37) included in an optical disk reader.

10. Method according to claim 8, characterised in that it comprises an additional stage according to which :

- prior to the decryption stage, the data (DATA) is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocerssor interface (37) included in a computer (40).

11. Method according to claim 8, characterised in that in the decryption stage the data (DATA) is systematically decrypted, whether said data is encrypted or not.

12. Method according to claim 8, characterised in that it comprises an additional stage according to which :

- a set of unprocessed data (B) and a set of decrypted data (D) are loaded into a computer (40), both sets of data originating from a set of data read in the disk (10).

13. Method according to claim 12, characterised in that loading is made alternately.

14. Method according to claim 12, characterised in that a set of unprocessed data (B) is composed of at last one

zone of unusable encrypted data (Bb), and a set of decrypted data (D) is composed of at least one zone of usable decrypted data (Da).

15. Method according to claim 12, characterised in that a set of unprocessed data (B) is composed of at least one zone of usable-non-encrypted data (Ba), and a set of decrypted data (D) is composed of at least one zone of unusable decrypted data (Dd).

16. Method according to claim 14 or 15, characterised in that it comprises an additional stage according to which:

- an executable code portion in a useful data zone including application data is executed.

17. Method according to claim 16, characterised in that it comprises an additional stage according to which :

- various data zones are interconnected, new data is loaded into the memory and a data zone is reconstituted with the aid of a set of links included in the executable code.

18. Disk reader device (30, 40) placed to read an optical data storage disk (10) as defined in claim 1, said device including an interface (37, 38) for exchanging data with the decryption module (20).

19. Method for protecting an optical data storage disk (10) comprising a decryption module (20) including :

- a memory (22) ;
- a cryptoprocessor (21), and
- data exchange means (IN_A, OUT_A, VCC_A, GRD_A),

the method including the following stages :

- an encryption stage in which the data is encrypted from at least one sole secret key (K1) so as to obtain encrypted data ;
- a writing stage in which the encrypted data are written in said optical disk (10), and
- a loading stage in which the key or keys is/are loaded into the memory (22) of the decryption module (20).

memory and reconstructing a data zone.

18. Optical disk according to one of claims 1 to 17, characterised in that the data (DATA) of the disk form at least one application written in high-level language.

19. Optical disk according to claim 18, characterised in that the application is partially or totally encrypted.

20. Method for protecting an optical disk (10) for storing data, characterised in that the method comprises stages according to which :

- data (DATA) of said disk (10) is decrypted with the aid of a secret key (K1) included in a memory (22) of a portable object (20) integrated in said disk and remaining inside said object during decryption,
- the data (DATA) of said disk (10) is exchanged between said portable object (20) and said disk by means of data exchange means (IN_A, OUT_A, VCC_A, GRD_A) integrated in said disk.

21. Method according to claim 20, characterised in that said portable object is a chip with an integrated circuit.

22. Method according to claim 20 or 21, characterised in that the decryption stage is carried out using a cryptoprocessor integrated in said portable object (20).

23. Method according to claim 22, characterised in that it comprises an additional stage according to which :

- prior to the decryption stage, the data (DATA) is modified into a format able to be understood by the cryptoprocessor via a cryptoprocessor (37) included in an optical disk reader.

24. Method according to claim 22, characterised in that it comprises an additional stage according to which :

- prior to the decryption stage, the data (DATA) is modified into a format able to be understood by the cryptoprocessor by means of a cryptoprocessor interface (37) included in a computer (40).

25. Method according to one of claims 20to 24,

characterised in that in the decryption stage the data (DATA) is decrypted systematically regardless of whether said data was originally encrypted or not.

26. Method according to one of claims 20 to 25, characterised in that it comprises an additional stage according to which :

- a set of unprocessed decrypted data (D) originating from a set of data read in the disk (10) is loaded into a computer (40).

27. Method according to claim 26, characterised in that loading is carried out alternately.

28. Method according to claim 26, characterised in that a set of unprocessed data (B) is composed of at least one zone of unusable encrypted data (Bb) and a set of decrypted data (D) is composed of at least one zone of usable decrypted data (Da).

29. Method according to claim 26, characterised in that a set of unprocessed data (B) is composed of at least one non-encrypted useful zone of data (Ba), and a set of decrypted data (D) is composed of at least one zone of unusable decrypted data (Dd).

30. Method according to claim 28 or 29, characterised in that it comprises an additional stage according to which :

- one executable code portion included in the useful data zone is executed including application data.

31. Method according to claim 30, characterised in that it comprises an additional stage according to which :

- various data zones are interconnected, new data is loaded into the memory and a data zone is reconstructed with the aid of a set of links included in the executable code.

32. Method according to one of claims 20 to 31, characterised in that it comprises an additional stage according to which :

- data is encrypted by means of a secret key (K1),
- said encrypted data is written in said disk (10).

33. Method according to one of claims 20 to 32, characterised in that it comprises data (DATA) forming at least one application written in high-level language.

34. Method according to claim 33, characterised in that the application is partially or totally encrypted.